Course : CISA, Certified IS Auditor, preparation for ISACA certification

Practical course - 5d - 35h00 - Ref. CKA
Price : 3400 € E.T.

4,2 / 5

This course enables you to prepare for the CISA® (Certified Information Systems Auditor) exam, by covering the entire CBK (Common Body of Knowledge) syllabus, the common core of security knowledge defined by ISACA® (Information Systems Audit and Control Association). This course is given in French, and the official materials used are in English.

Teaching objectives

At the end of the training, the participant will be able to:

- Prepare for the CISA certification exam, ISACA Certified Security Auditor
- Understand the five main areas of CISA® certification
- Understand IS auditing and IT governance concepts

Intended audience

IT/IS auditors, control, assurance and information security professionals.

Prerequisites

Five or more years' experience in IS/IT audit, control, assurance or security.

Course schedule

PARTICIPANTS

IT/IS auditors, control, assurance and information security professionals.

PREREQUISITES

Five or more years' experience in IS/IT audit, control, assurance or security.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant’s academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they’ve developed.

1 Area 1: information systems audit process

- IS auditing standards, guidelines and codes of ethics.
- Business processes.
- Types of controls.
- Risk-based audit planning.
- Types of audits and evaluations.
- Audit project management.
- Sampling methodology.
- Techniques for collecting audit evidence.
- Data analysis.
- Reporting and communication techniques.
- Quality assurance and audit process improvement.

2 Area 2: Information systems governance and management

- IT governance and IT strategy.
- IT-related executives.
- IT standards, policies and procedures.
- Organizational structure.
- Enterprise architecture.
- Enterprise risk management.
- Maturity models.
- Laws, regulations and industry standards affecting the organization.
- IT resource management.
- Procurement and management of IT service providers.
- IT performance monitoring and reporting.
- Information technology quality assurance and management.

3 Area 3: IS acquisition, design and implementation

- Governance and project management.
- Profitability and feasibility analysis.
- Systems development methodologies.
- Identification and design of controls.
- Test methodologies.
- Configuration and version management.
- System migration, infrastructure deployment and data conversion.
- Post-implementation review.

4 Area 4: Operation, maintenance and support of information systems

- Common technological components.
- IT asset management.
- Task planning and automation of production processes.
- System interfaces.
- End-user computing.
- Data governance.
- System performance management.
- Problem and incident management.
- Change, configuration, version and patch management.
- IT service level management.
- Database management.
- Business Impact Analysis (BIA).
- System resilience.
- Data backup, storage and restoration.
- Business continuity plan (BCP).
- Disaster recovery plans (DRP).

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

5 Area 5: Protecting information assets

- Information security frameworks, standards and guidelines.
- Privacy principles.
- Physical access and environmental controls.
- Identity and access management.
- Network and endpoint security.
- Data classification.
- Data encryption and encryption-related techniques.
- Public Key Infrastructure (PKI).
- Web-based communication techniques.
- Virtualized environments.
- Mobile, wireless and Internet of Things (IoT) devices.
- Safety training and awareness programs.
- Methods and techniques for attacking information systems.
- Security testing tools and techniques.
- Safety control tools and techniques.
- Incident response management.
- Evidence gathering and forensics.

Options

Certification : 780 € HT

The exam, available online and off-line, consists of 150 questions to be completed in 4 hours. CISA certification is recognized worldwide.

Dates and locations

REMOTE CLASS
2026 : 16 Mar., 29 June, 12 Oct., 14 Dec.

PARIS LA DÉFENSE
2026 : 22 June, 5 Oct., 14 Dec.